18 years of DNSSEC adoption measurements: How far have we come?

https://cs.rkempe.ca
rebeccakempe@cmail.carleton.ca

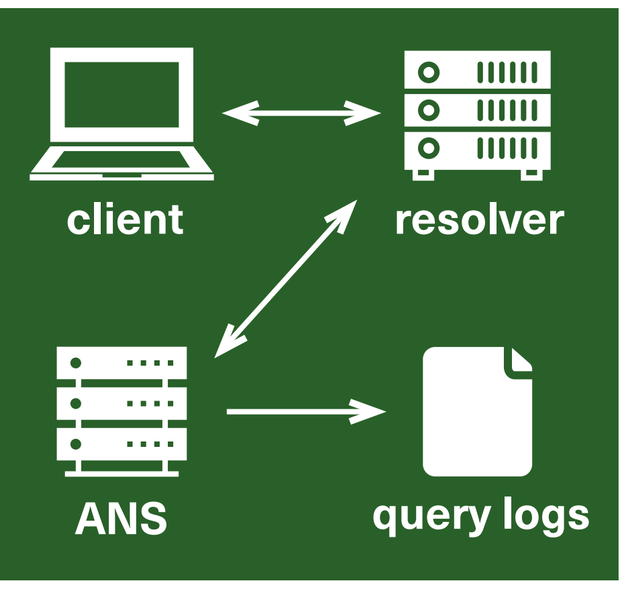
Rebecca Kempe*, AbdelRahman Abdou*
*School of Computer Science, Carleton University, Ottawa, ON

Carleton University

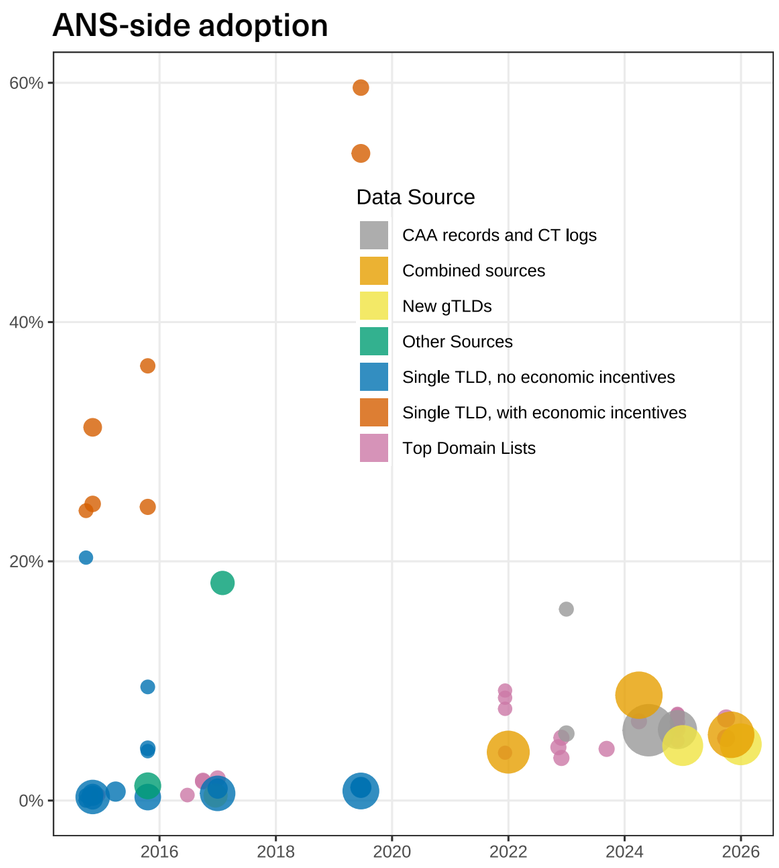
- The DNS Security Extensions (DNSSEC) are the most effective mitigation against cache poisoning attacks.
- Consensus is that adoption remains low, but no single source of longitudinal data currently exists.
- Existing DNSSEC adoption studies use different methodologies, which makes direct comparisons difficult.
- We analyze, classify, and chart 100+ adoption measurements extracted from 48 papers and reports.
- We find major inconsistencies in the resolver-side results and introduce a framework to help compare measurements and specify how they were obtained.

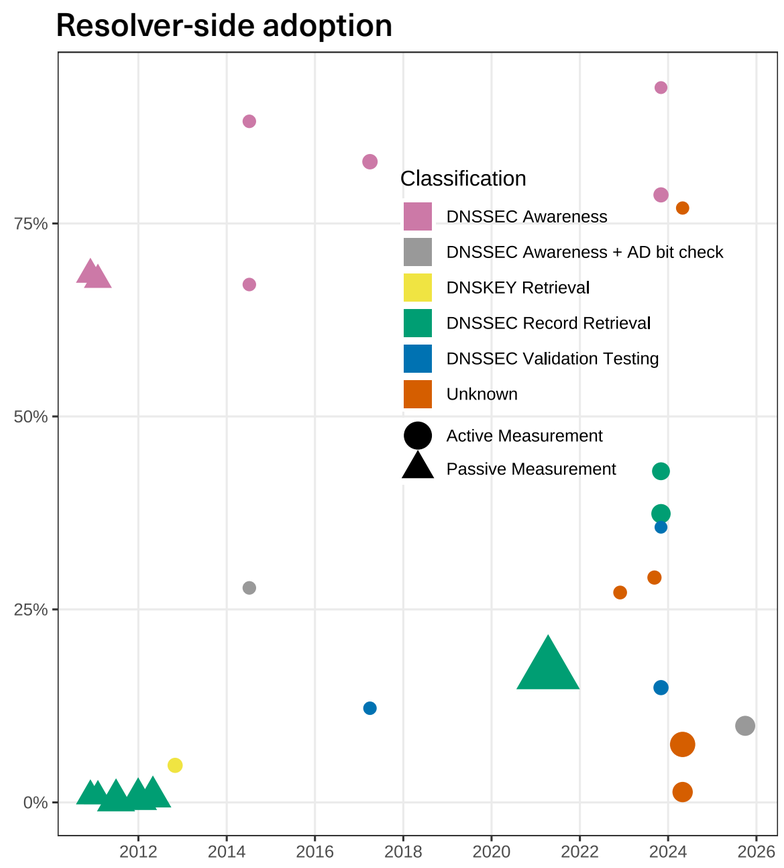
Five ways DNSSEC adoption is currently measured

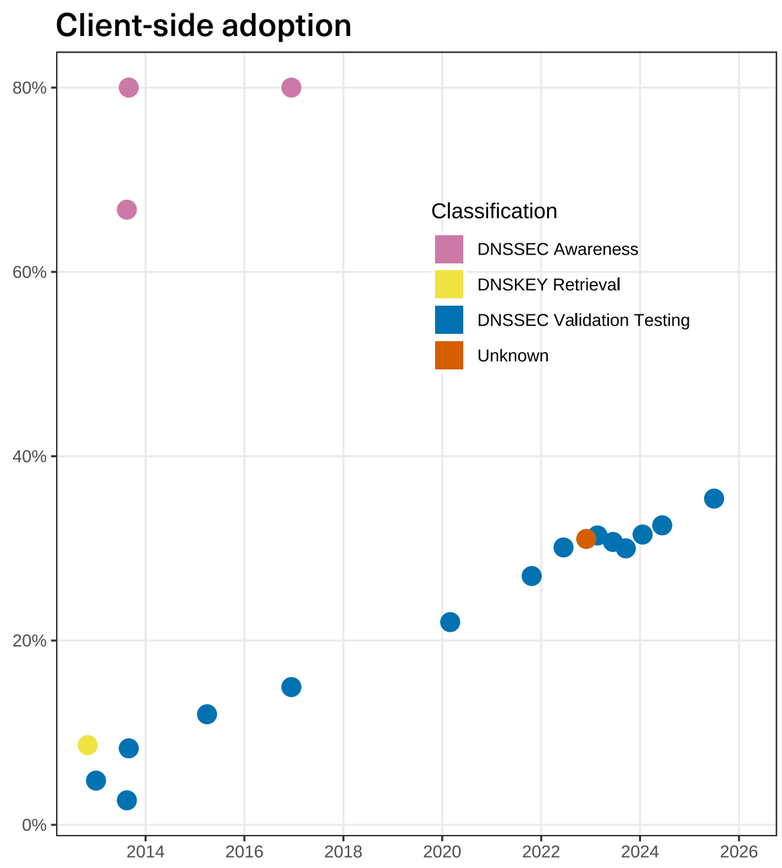
1. **Authoritative name server (ANS)-side adoption (a.k.a. zone signing):**
   What proportion of domains are DNSSEC-signed?
2. **Resolver-side adoption (a.k.a. resolver validation):**
   What proportion of resolvers are DNSSEC-validating?
3. **Client-side adoption (a.k.a. client-side protection or usage):**
   What proportion of clients are either using DNSSEC validation themselves or protected by a validating resolver?
4. What proportion of DNS query traffic is being generated by validating resolvers?
5. What proportion of DNS queries are for signed domains?



Is DNSSEC adoption increasing? It depends...







The compiled data suggest that overall ANS-side adoption has grown from around 0.5% in 2014 to around 5% in 2026, and client-side adoption has grown from around 5% in 2012 to around 35% in 2025. However, few conclusions can be drawn from the resolver-side data. For the ANS-side and resolver-side charts, a larger point indicates a bigger sample.

Our measurement classification groupings, explained

ANS-side measurement types

Signature Existence: Checks whether the zone contains RRSIGs for at least one type of resource record.

DNSKEY Existence: Checks whether the zone contains a DNSKEY RRset.

DNSKEY Existence + Signature: Checks whether the zone contains a DNSKEY RRset and whether that RRset is signed.

DS Record Existence: Checks whether the parent zone contains a DS record for this zone.

Zone Correctness: Checks whether the zone was correctly signed.

Resolver-side measurement types

DNSSEC Awareness: Checks if the DO bit is set and (optionally) if the resolver returns RRSIGs to the client.

DNSSEC Awareness + AD bit check: Checks if the resolver informs the client (by setting the AD bit) when it has validated a response.

DNSKEY Retrieval: Checks if the resolver retrieves DNSKEY records for the zone.

DNSSEC Record Retrieval: Checks whether the resolver retrieves all necessary records to validate the zone.

DNSSEC Validation Testing: Checks if the resolver fails on queries to bogus zones.

Key observations

- We conclude that **DNSSEC adoption is increasing.** However, it is unclear whether client-side adoption is increasing because more resolvers are validating or if this is a consequence of DNS centralization.
- The **resolver-side data are so scattered that we cannot draw conclusions from aggregating them.** We believe that this is due to major differences in the data sources and measurement methodologies.
- For each adoption metric, there are multiple measurement methods with varying levels of precision. However, **many authors do not explain their methodology, making it impossible to compare results.**
- Some papers directly compare, or even combine, client-side and resolver-side measurements, despite the fact that **they mean different things and are not interchangeable.**
- Many papers that report on DNSSEC adoption **are primarily about another topic** (e.g., attacks, algorithm agility or DNSSEC misconfigurations) and include adoption measurements as **contextual information.**

References & data sources:

- Academic conference and journal papers
- Government (e.g., EU, US) reports
- Industry reports and whitepapers
- Technical reports and academic theses
- APNIC blog posts and presentations

Our key words were “DNSSEC deployment,” “DNSSEC adoption,” and “DNSSEC measurement.” We also included adjacent papers when they were relevant. Whenever possible, we used the author-reported adoption statistics; otherwise, we did our own calculations based on the data in the reference.